REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 16-24 and 26-30 are pending in the present application. Claims 1-15 are previously cancelled and Claims 16, 23, 24 and 26-30 are amended and Claim 25 is cancelled without prejudice or disclaimer by the present amendment. Support for amendments to the claims can be found in the disclosure as originally filed. Thus, no new matter is added.

In the outstanding Action, Claims 16-19, 21, 22, 24-26 and 28 were rejected under 35 U.S.C. §103(a) as unpatentable over Kanno et al. (U.S. Pat. Pub. No. 2004/0064738, herein "Kanno") in view of Bang et al. (KR Pat Pub No. 10-2004-0036228, herein "Bang"); Claim 20 was rejected under 35 U.S.C. §103(a) as unpatentable over Kanno and Bang in view of Ioele et al. (U.S. Pat. No. 7,007,229, herein "Ioele"); Claim 23 was rejected under 35 U.S.C. §103(a) as unpatentable over Kanno and Bang in view of Patrick et al. (U.S. Pat. No. 7,310,684, herein "Patrick"); and Claim 27 was rejected under 35 U.S.C. §103(a) as unpatentable over Kanno and Bang in view of Costa et al. (U.S. Pat. No. 2007/0006314, herein "Costa").

Addressing now the rejection of Claims 16-19, 21, 22, 24-26 and 28 under 35 U.S.C. §103(a) as unpatentable over Kanno and Bang, Applicants respectfully traverse this assertion.

Amended Claim 16 recites,

> A denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system comprising:
>
> a monitoring device that monitors each packet transmitted to the communication device and includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device;
>
> a performance measuring device that measures response performance of the communication device by sending a response request message and is separate from the

> communication device and the monitoring device, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device; and
>
> an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device, the attack determining device including an effects determining unit that determines whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, and
>
> the effects determining unit determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Claim 28 recites a corresponding method claim.

Kanno describes a server computer protection apparatus which protects a server against DoS attacks by counting the number of incoming data requests and the number of outgoing data supplies and cutting off the data requests when an imbalance between the two is too high.

However, Kanno does not describe or suggest, among other things, a performance measuring device that measures response performance of the communication device by sending a response request message and is separate from the communication device and the monitoring device, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device, as is recited in Claim 16.

The outstanding Action states on page 2 that element 908 in Figure 9 of Kanno describes the claimed performance measuring device. Applicants respectfully traverse this assertion. Specifically, the processing situation reception unit 908 of Kanno is simply a

device that receives processing situation information from the server 104. This element does not measure response performance of the communication device by sending a response request message.

Thus, Kanno cannot be asserted as describing the performance measuring device recited in Claim 16.

Nevertheless, the outstanding Action cites Bang as curing the deficiencies of Kanno with regard to the claimed invention.

Bang describes a system for detecting harmful traffic, tracing the source of the harmful traffic and cutting off the source of the harmful traffic. Specifically, Bang describes monitoring changes in traffic flow. When the change in traffic flow exceeds a certain threshold, the system detects the source of the traffic and cuts it off.

However, Bang never describes or suggests a performance measuring device that measures response performance of the communication device by sending a response request message and is separate from the communication device and the monitoring device, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device, as is recited in Claim 16.

Thus, the combination of Kanno and Bang cannot be asserted as describing the performance measuring device recited in Claim 16.

Moreover, the combination of Kanno and Bang does not describe or suggest an attack determining device that is connected to and performs communication with ***both the monitoring device and the performance measuring device***, the attack determining device including an effects determining unit that determines whether the communication device has received the denial-of-service attack, ***using both the traffic abnormality information and the performance abnormality information***.

The outstanding Action cites element 103 of Kanno as disclosing the attack determining device recited in Claim 16, however, Applicants respectfully traverse this assertion and submit that this reference does not describe or render obvious using two different methods in concert to determine whether a communication device is a recipient of the denial-of-service (DoS) attack.

Furthermore, DoS attacks often transmit a large number of packets to a service which a targeted server does not offer. Kanno is unable to properly detect such an attack because Kanno, in which attack packets and responses are not sufficiently counted, only detects the DoS attacks when packets are transmitted to services actually offered by the server.

In contrast, the claimed invention uses a detecting method based on performance abnormality, which actively measures performance of services offered by the server, along with monitoring of traffic abnormality that detects abnormality of packets for services which are not offered by the server. As a result, DOS attacks in which a large number of packets are transmitted to a service, which the targeted served does not offer, can be detected. However, this feature is not provided by the Kanno or the further cited Bang reference. Therefore, the claimed invention is not obvious from the cited references.

In addition, Applicants note that because of the way in which Kanno detects the DoS attacks, Kanno has a problem of erroneously detecting certain performance abnormalities as DoS attacks when no attack is in fact being made. For instance, issues such as a failure of a hard disk drive in the server or programming bugs are erroneously detected as DoS attacks.

Moreover, with regard to the combination of Kanno and Bang, this combination cannot be relied on to render obvious the features of amended Claims 16 and 28. Specifically, the combination of Kanno and Bang fails to describe or render obvious that the effects determining unit determines that the communication device has received the denial-of-service attack, ***when it is determined that one of the traffic abnormality information and***

the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information as is recited in the claimed invention.

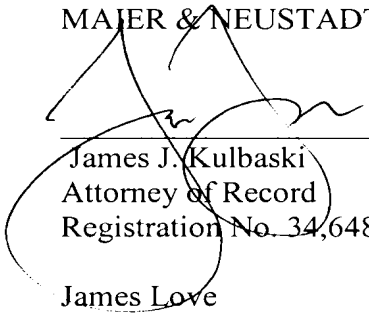
In other words, the claimed invention collects the traffic abnormality information and the performance abnormality information and specifies the cause and effect based on the occurrence time and makes a determination regarding whether the device has received the DoS attack. Therefore, the claimed invention is not only not described or suggested in either Kanno or Bang, but also is not rendered obvious by the combination of Kanno and Bang.

Accordingly, Applicants respectfully submit that Claim 16 and similarly Claim 28, and claims depending therefrom, patentably distinguish over Kanno and Bang considered individually or in combination.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

James Love
Registration No. 58,421

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\JL\288056US\288056US_AM(11.24.2008).DOC